Chapter One

THE ADVENT OF NETWAR (REVISITED)[1]

John Arquilla and David Ronfeldt

Editors' abstract. This introductory chapter provides a reprise of many of the points we have made about the netwar concept since 1993. In this book, we depict netwar as having two major faces, like the Roman god Janus—one dominated by terrorists and criminals that is quite violent and negative, and another evinced by social activists that can be militant but is often peaceable and even promising for societies. Indeed, the book is structured around this theme.

The information revolution is altering the nature of conflict across the spectrum. We call attention to two developments in particular. First, this revolution is favoring and strengthening network forms of organization, often giving them an advantage over hierarchical forms. The rise of networks means that power is migrating to nonstate actors, because they are able to organize into sprawling multiorganizational networks (especially "all-channel" networks, in which every node is connected to every other node) more readily than can traditional, hierarchical, state actors. This means that conflicts may increasingly be waged by "networks," perhaps more than by "hierarchies." It also means that whoever masters the network form stands to gain the advantage.

Second, as the information revolution deepens, the conduct and outcome of conflicts increasingly depend on information and communications. More than ever before, conflicts revolve around "knowledge"

[1]Our netwar concept predates, and should not be confused with, the U.S. military's network warfare simulation (NETWARS) system.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2001		**00-00-2001 to 00-00-2001**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Advent of Netwar (Revisited)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Graduate School of Operational and Information Sciences,Department of Defense Analysis,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
In Networks and Netwars: The Future of Terror, Crime, and Militancy (John Arquilla and David Ronfeldt eds.), Santa Monica, CA: RAND, 1993-2003

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

and the use of "soft power."[2] Adversaries are learning to emphasize "information operations" and "perception management"—that is, media-oriented measures that aim to attract or disorient rather than coerce, and that affect how secure a society, a military, or other actor feels about its knowledge of itself and of its adversaries. Psychological disruption may become as important a goal as physical destruction.

These propositions cut across the entire conflict spectrum. Major transformations are thus coming in the nature of adversaries, in the type of threats they may pose, and in how conflicts can be waged. Information-age threats are likely to be more diffuse, dispersed, multidimensional nonlinear, and ambiguous than industrial-age threats. Metaphorically, then, future conflicts may resemble the Oriental game of *Go* more than the Western game of chess. The conflict spectrum will be remolded from end to end by these dynamics.

A CONCEPT AND ITS BRIEF HISTORY

Back in 1992, while first wondering about such propositions and writing about *cyberwar* as a looming mode of military conflict, we thought it would be a good idea to have a parallel concept about information-age conflict at the less military, low-intensity, more social end of the spectrum. The term we coined was *netwar*, largely because it resonated with the surety that the information revolution favored the rise of network forms of organization, doctrine, and strategy. Through netwar, numerous dispersed small groups using the latest communications technologies could act conjointly across great distances. We had in mind actors as diverse as transnational terrorists, criminals, and even radical activists. Some were already moving from hierarchical to new information-age network designs.

We fielded the netwar concept in our first journal article, "Cyberwar Is Coming" (1993), then provided a full exposition in our RAND report, *The Advent of Netwar* (1996). Additional insights were advanced in the concluding chapter of our book, *In Athena's Camp* (1997). Elaborations appeared in multiauthored RAND volumes on *The Zapatista*

[2]The concept of soft power was introduced by Nye (1990), and further elaborated in Nye and Owens (1996).

"Social Netwar" in Mexico (Ronfeldt et al., 1998) and *Countering the New Terrorism* (Lesser et al., 1999). Our study *The Emergence of Noopolitik: Toward an American Information Strategy* (1999) observed that many socially minded nongovernmental organizations (NGOs) were already using netwar strategies to enhance their soft power. Our recent study *Swarming and the Future of Conflict* (2000) is mainly about developing a new military doctrine for wielding "hard" power, but it generally advances our view that swarming is likely to become the dominant approach to conflict across the spectrum, including among netwar actors. While the Zapatista study provided early evidence for this, short opinion pieces on the military war in Kosovo (1999) and the activist "Battle for Seattle" (1999) identified new cases.[3]

As these writings have spread, the netwar concept has struck a chord with a growing number of theorists, futurists, journalists, and practitioners. In forward-looking books, scholars as diverse as Manuel Castells (1997), Chris Hables Gray (1997), and David Brin (1998) have used the concept for discussing trends at the mostly nonmilitary end of the conflict spectrum. For several years, a web site maintained by Jason Wehling carried a wide range of articles about netwar, social activism, and information-age conflict, leading off with a paper he had written about the netwar concept (1995). Meanwhile, interesting flurries of discussion about netwar arose on email lists related to the Zapatista movement in Mexico following the armed uprising in January 1994. Harry Cleaver's writings (e.g., 1995, 1998, 1999) are particularly illuminating. They show that Mexico became a laboratory for the emergence of a new, non-Leninist model of radicalism. The Zapatista leader, Subcomandante Marcos, even averred in 1999 that netwar described the Zapatista movement, and that *counternetwar* instructed the strategy of its military and paramilitary opponents. For its part, the high command of the Mexican military also espoused admiration for the concept during 2000.[4] Also in 2000, a leader of the International Campaign to Ban Landmines (ICBL), Jody Williams, remarked in a

[3]John Arquilla and David Ronfeldt, "Need for Networked, High-Tech Cyberwar," *Los Angeles Times*, June 20, 1999, pp. A1, A6; John Arquilla and David Ronfeldt, "A Win for Netwar in Seattle," December 1999, posted on the web site for the Highlands Forum.

[4]Both the Zapatista and the Mexican army leadership had read the RAND report analyzing the Zapatista movement as a case of social netwar (Ronfeldt et al., 1998).

radio interview that she had heard that RAND researchers were developing the netwar concept to help governments control movements like the ICBL. Elsewhere, the concept cropped up in marginal rants and ruminations by militants associated with various left-wing, right-wing, and eclectic religious movements who posted on Usenet discussion groups.

Meanwhile, officials and analysts in U.S. and European government, military, and police circles began showing an interest in the concept. They were finding it difficult to deal with terrorists, criminals, and fanatics associated with militias and extremist single-issue movements, largely because these antagonists were organizing into sprawling, loose, "leaderless" networks, overcoming their former isolated postures as stand-alone groups headed by "great men." U.S. and European officials realized that these troublesome trends put a premium on interagency communication and coordination, for everything from intelligence sharing to tactical operations. But this implied a degree of cross-jurisdictional and international networking, especially for intelligence sharing, that is difficult for state hierarchies to accomplish. The concepts of netwar and counternetwar attracted some interest because they had a potential for motivating officials to build their own networks, as well as hybrids of hierarchies and networks, to deal with the networked organizations, doctrines, and strategies of their information-age adversaries. A special issue of the journal *Studies in Conflict and Terrorism* on "Netwar Across the Spectrum of Conflict" (1999) may have helped heighten awareness of this.[5]

Our formulation of the netwar concept has always emphasized the organizational dimension. But we have also pointed out that an organizational network works best when it has the right doctrinal, technological, and social dynamics. In our joint work, we have repeatedly insisted on this. However, writers enamored of the flashy, high-tech aspects of the information revolution have often depicted netwar (and cyberwar) as a term for computerized aggression waged via stand-off attacks in cyberspace—that is, as a trendy synonym for in-

[5]This special issue was partly assembled and edited by David Ronfeldt. Some text in this section comes from his introduction to that issue.

fowar, information operations, "strategic information warfare," Internet war, "hacktivism," cyberterrorism, cybotage, etc.[6]

Thus, in some quarters, the Serb hacks of NATO's web site in 1999 were viewed as netwar (or cyberwar). Yet, little was known about the perpetrators and the nature of their organization; if they amounted to just a few, clever, government-sponsored individuals operating from a site or two, then the netwar dimensions of this case were minimal, and it was just a clever instance of minor cybotage. This case also speaks to another distortion: These Serbs (presumably they were Serbs) aimed to bring a piece of "the Net" down. Yet, in a full-fledged ethnonationalist, terrorist, criminal, or social netwar, the protagonists may be far more interested in keeping the Net up. They may benefit from using the Internet and other advanced communications services (e.g., fax machines and cellular telephones) for purposes that range from coordinating with each other and seeking recruits, to projecting their identity, broadcasting their messages to target audiences, and gathering intelligence about their opponents.

With respect to Serbia, then, a better case of netwar as we define it was the effort by Serbia's reformist Radio B-92, along with a supportive network of U.S. and European government agencies and NGOs, to broadcast its reportage back into Serbia over the Internet, after B-92's transmitters were shut down by the Milosevic regime in 1998 and again in 1999. For a seminal case of a worldwide netwar, one need look no further than the ICBL. This unusually successful movement consists of a loosely internetted array of NGOs and governments, which rely heavily on the Internet for communications. Through the personage of one of its many leaders, Jody Williams, this netwar won a well-deserved Nobel peace prize.[7]

---

[6]For an interesting paper by a leading proponent of hacktivism, see Wray (1998).

[7]See speech by Jody Williams accepting the Nobel Peace Prize in 1997, www.wagingpeace.org/articles/nobel_lecture_97_williams.html; and the speech she gave at a gathering of recipients at the University of Virginia in 1998, www.virginia.edu/nobel/transcript/jwilliams.html, as well as Williams and Goose (1998).

DEFINING NETWAR[8]

To be precise, the term netwar refers to an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an internetted manner, often without a precise central command. Thus, netwar differs from modes of conflict and crime in which the protagonists prefer to develop formal, stand-alone, hierarchical organizations, doctrines, and strategies as in past efforts, for example, to build centralized movements along Leninist lines. Thus, for example, netwar is about the Zapatistas more than the Fidelistas, Hamas more than the Palestine Liberation Organization (PLO), the American Christian Patriot movement more than the Ku Klux Klan, and the Asian Triads more than the Cosa Nostra.[9]

The term *netwar* is meant to call attention to the prospect that network-based conflict and crime will become major phenomena in the decades ahead. Various actors across the spectrum of conflict and crime are already evolving in this direction. This includes familiar adversaries who are modifying their structures and strategies to take advantage of networked designs—e.g., transnational terrorist groups, black-market proliferators of weapons of mass destruction (WMD), drug and other crime syndicates, fundamentalist and ethnonationalist movements, intellectual-property pirates, and immigration and refugee smugglers. Some urban gangs, back-country militias, and militant single-issue groups in the United States have also been developing netwar-like attributes. The netwar spectrum also includes a new generation of revolutionaries, radicals, and activists who are beginning to create information-age ideologies, in which identities and

[8]This section reiterates but also updates our earlier formulations about the nature of netwar (notably those in Arquilla and Ronfeldt, 1996; Ronfeldt et al., 1998; and Arquilla, Ronfeldt, and Zanini, 1999). Readers who are already familiar with this work may prefer to skip this section.

[9]This is just a short exemplary statement. Many other examples could be noted. Instead of Hamas, for example, we might mention the Committee for the Defense of Legitimate Human Rights (CDLHR), an anti-Saudi organization based in London.

loyalties may shift from the nation state to the transnational level of "global civil society." New kinds of actors, such as anarchistic and nihilistic leagues of computer-hacking "cyboteurs," may also engage in netwar.

Many—if not most—netwar actors will be nonstate, even stateless. Some may be agents of a state, but others may try to turn states into *their* agents. Also, a netwar actor may be both subnational and transnational in scope. Odd hybrids and symbioses are likely. Furthermore, some bad actors (e.g., terrorist and criminal groups) may threaten U.S. and other nations' interests, but other actors (e.g., NGO activists in Burma or Mexico) may not—indeed, some actors who at times turn to netwar strategies and tactics, such as the New York–based Committee to Protect Journalists (CPJ), may have salutary liberalizing effects. Some actors may aim at destruction, but more may aim mainly at disruption and disorientation. Again, many variations are possible.

The full spectrum of netwar proponents may thus seem broad and odd at first glance. But there is an underlying pattern that cuts across all variations: *the use of network forms of organization, doctrine, strategy, and technology attuned to the information age.*

More About Organizational Design

In an archetypal netwar, the protagonists are likely to amount to a set of diverse, dispersed "nodes" who share a set of ideas and interests and who are arrayed to act in a fully internetted "all-channel" manner. In the scholarly literature (e.g., Evan, 1972), networks come in basically three types or topologies (see Figure 1.1):

- The *chain* or line network, as in a smuggling chain where people, goods, or information move along a line of separated contacts, and where end-to-end communication must travel through the intermediate nodes.
- The *hub*, star, or wheel network, as in a franchise or a cartel where a set of actors are tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other.

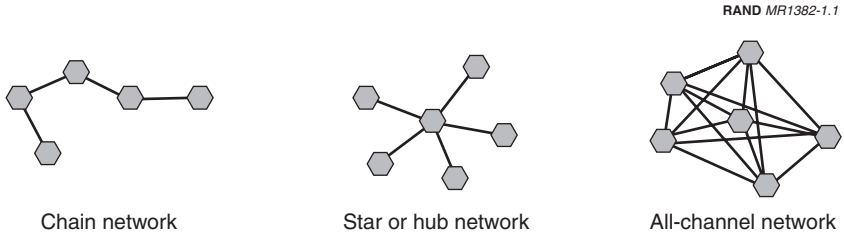

Figure 1.1—Three Basic Types of Networks

- The *all-channel* or full-matrix network, as in a collaborative network of militant peace groups where everybody is connected to everybody else.

Each node in the diagrams may refer to an individual, a group, an organization, part of a group or organization, or even a state. The nodes may be large or small, tightly or loosely coupled, and inclusive or exclusive in membership. They may be segmentary or specialized—that is, they may look alike and engage in similar activities, or they may undertake a division of labor based on specialization. The boundaries of the network, or of any node included in it, may be well-defined, or blurred and porous in relation to the outside environment. Many variations are possible.

Each type may be suited to different conditions and purposes, and all three may be found among netwar-related adversaries—e.g., the chain in smuggling operations; the hub at the core of terrorist and criminal syndicates; and the all-channel type among militant groups that are highly internetted and decentralized. There may also be hybrids of the three types, with different tasks being organized around different types of networks. For example, a netwar actor may have an all-channel council or directorate at its core but use hubs and chains for tactical operations. There may also be hybrids of network and hierarchical forms of organization. For example, traditional hierarchies may exist inside particular nodes in a network. Some actors may have a hierarchical organization overall but use network designs for tactical operations; other actors may have an all-channel network design

overall but use hierarchical teams for tactical operations. Again, many configurations are possible, and it may be difficult for an analyst to discern exactly what type characterizes a particular network.

Of the three network types, the all-channel has been the most difficult to organize and sustain, partly because it may require dense communications. But it is the type that gives the network form its new, high potential for collaborative undertakings and that is gaining new strength from the information revolution. Pictorially, an all-channel netwar actor resembles a geodesic "Bucky ball" (named for Buckminster Fuller); it does not look like a pyramid. The organizational design is flat. Ideally, there is no single, central leadership, command, or headquarters—no precise heart or head that can be targeted. The network as a whole (but not necessarily each node) has little to no hierarchy; there may be multiple leaders. Decisionmaking and operations are decentralized, allowing for local initiative and autonomy. Thus the design may sometimes appear acephalous (headless), and at other times polycephalous (Hydra-headed).[10]

The capacity of this design for effective performance over time may depend on the existence of shared principles, interests, and goals—perhaps an overarching doctrine or ideology—which spans all nodes and to which the members subscribe in a deep way. Such a set of principles, shaped through mutual consultation and consensus-building, can enable members to be "all of one mind" even though they are dispersed and devoted to different tasks. It can provide a central ideational and operational coherence that allows for tactical decentralization. It can set boundaries and provide guidelines for decisions and actions so that the members do not have to resort to a hierarchy because "they know what they have to do."[11]

The network design may depend on having an infrastructure for the dense communication of functional information. This does not mean that all nodes must be in constant communication; that may not

[10]The structure may also be cellular. However, the presence of "cells" does not necessarily mean a network exists. A hierarchy can also be cellular, as is the case with some subversive organizations.

[11]The quotation is from a doctrinal statement by Beam (1992) about "leaderless resistance," which has strongly influenced right-wing white-power groups.

make sense for a secretive, conspiratorial actor. But when communication is needed, the network's members must be able to disseminate information promptly and as broadly as desired within the network and to outside audiences.

In many respects, then, the archetypal netwar design corresponds to what earlier analysts (Gerlach, 1987, p. 115, based on Gerlach and Hine, 1970) called a "segmented, polycentric, ideologically integrated network" (SPIN):

> By segmentary I mean that it is cellular, composed of many different groups. . . . By polycentric I mean that it has many different leaders or centers of direction. . . . By networked I mean that the segments and the leaders are integrated into reticulated systems or networks through various structural, personal, and ideological ties. Networks are usually unbounded and expanding. . . . This acronym [SPIN] helps us picture this organization as a fluid, dynamic, expanding one, spinning out into mainstream society.[12]

Caveats About the Role of Technology

Netwar is a result of the rise of network forms of organization, which in turn is partly a result of the computerized information revolution.[13] To realize its potential, a fully interconnected network requires a capacity for constant, dense information and communications flows, more so than do other forms of organization (e.g., hierarchies). This capacity is afforded by the latest information and communication technologies—cellular telephones, fax machines, electronic mail (email), web sites, and computer conferencing. Such technologies are highly advantageous for netwar actors whose constituents are geographically dispersed.

---

[12]The SPIN concept is a precursor of the netwar concept. Proposed by Luther Gerlach and Virginia Hine in the 1960s to depict U.S. social movements, it anticipates many points about network forms of organization, doctrine, and strategy that are now coming into focus in the analysis not only of social movements but also of some terrorist, criminal, ethnonationalist, and fundamentalist organizations.

[13]For explanation of this point, see Ronfeldt (1996), Arquilla and Ronfeldt (1996), and other sources cited in those documents.

But two caveats are in order. First, the new technologies, however enabling for organizational networking, are not absolutely necessary for a netwar actor. Older technologies, like human couriers, and mixes of old and new systems may do the job in some situations. The late Somali warlord, Mohamed Farah Aidid, for example, proved very adept at eluding those seeking to capture him while at the same time retaining full command and control over his forces by means of runners and drum codes (see Bowden, 1999). Similarly, the first Chechen War (1994–1996), which the Islamic insurgents won, made wide use of runners and old communications technologies like ham radios for battle management and other command and control functions (see Arquilla and Karasik, 1999). So, netwar may be waged in high-, low-, or no-tech fashion.

Second, netwar is not simply a function of "the Net" (i.e., the Internet); it does not take place only in "cyberspace" or the "infosphere." Some *battles* may occur there, but a *war's* overall conduct and outcome will normally depend mostly on what happens in the "real world"—it will continue to be, even in information-age conflicts, generally more important than what happens in cyberspace or the infosphere.[14]

Netwar is not solely about Internet war (just as cyberwar is not just about "strategic information warfare"). Americans have a tendency to view modern conflict as being more about technology than organization and doctrine. In our view, this is a misleading tendency. For example, social netwar is more about a doctrinal leader like Subcomandante Marcos than about a lone, wild computer hacker like Kevin Mitnick.

[14]This point was raised specifically by Paul Kneisel, "Netwar: The Battle over Rec.Music.White-Power," *ANTIFA INFO-BULLETIN*, Research Supplement, June 12, 1996, which is available on the Internet. He analyzes the largest vote ever taken about the creation of a new Usenet newsgroup—a vote to prevent the creation of a group that was ostensibly about white-power music. He concludes that "The *war* against contemporary fascism will be won in the 'real world' off the net; but *battles* against fascist netwar are fought and won on the Internet." His title is testimony to the spreading usage of the term *netwar*.

A Capacity for Swarming, and the Blurring of Offense and Defense

This distinctive, often ad-hoc design has unusual strengths, for both offense and defense. On the offense, networks tend to be adaptable, flexible, and versatile vis-à-vis opportunities and challenges. This may be particularly the case where a set of actors can engage in *swarming*. Little analytic attention has been given to swarming, [15] which is quite different from traditional mass- and maneuver-oriented approaches to conflict. Yet swarming may become the key mode of conflict in the information age (Arquilla and Ronfeldt, 2000, and Edwards, 2000), and the cutting edge for this possibility is found among netwar protagonists.

Swarming is a seemingly amorphous, but deliberately structured, coordinated, strategic way to strike from all directions at a particular point or points, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions. This notion of "force and/or fire" may be literal in the case of military or police operations, but metaphorical in the case of NGO activists, who may, for example, be blocking city intersections or emitting volleys of emails and faxes. Swarming will work best—perhaps it will only work—if it is designed mainly around the deployment of myriad, small, dispersed, networked maneuver units. Swarming occurs when the dispersed units of a network of small (and perhaps some large) forces converge on a target from multiple directions. The overall aim is *sustainable pulsing*—swarm networks must be able to coalesce rapidly and stealthily on a target, then dissever and redisperse, immediately ready to recombine for a new pulse. The capacity for a "stealthy approach" suggests that, in netwar, attacks are more likely to occur in "swarms" than in more traditional "waves." The Chechen resistance to the Russian army and the Direct Action Network's operations in the anti–World Trade Organization "Battle of Seattle" both provide excellent examples of swarming behavior.

[15]The first mention of "swarm networks" we encountered was in Kelly (1994). A recent discussion, really about "swarm intelligence" rather than swarm networks, is in Bonabeau, Dorigo, and Theraulaz (1999).

Swarming may be most effective, and difficult to defend against, where a set of netwar actors do not "mass" their forces, but rather engage in dispersion and "packetization" (for want of a better term). This means, for example, that drug smugglers can break large loads into many small packets for simultaneous surreptitious transport across a border, or that NGO activists, as in the case of the Zapatista movement, have enough diversity in their ranks to respond to any discrete issue that arises—human rights, democracy, the environment, rural development, whatever.

In terms of their defensive potential, networks tend to be redundant and diverse, making them robust and resilient in the face of attack. When they have a capacity for interoperability and shun centralized command and control, network designs can be difficult to crack and defeat as a whole. In particular, they may defy counterleadership targeting—a favored strategy in the drug war as well as in overall efforts to tamp organized crime in the United States. Thus, whoever wants to attack a network is limited—generally, only portions of a network can be found and confronted. Moreover, the deniability built into a network affords the possibility that it may simply absorb a number of attacks on distributed nodes, leading an attacker to believe the network has been harmed and rendered inoperable when, in fact, it remains viable and is seeking new opportunities for tactical surprise.

The difficulty of dealing with netwar actors deepens when the lines between offense and defense are blurred, or blended. When *blurring* is the case, it may be difficult to distinguish between attacking and defending actions, particularly where an actor goes on the offense in the name of self-defense. For example, the Zapatista struggle in Mexico demonstrates anew the blurring of offense and defense. The *blending* of offense and defense will often mix the strategic and tactical levels of operations. For example, guerrillas on the defensive strategically may go on the offense tactically, as in the war of the *mujahideen* in Afghanistan during the 1980s, and in both recent Chechen wars with the Russians.

Operating in the Seams

The blurring of offense and defense reflects another feature of netwar (albeit one that is exhibited in many other policy and issue areas): It tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal. This makes it difficult if not impossible for a government to assign responsibility to any single agency—e.g., military, police, or intelligence—to be in charge of responding.

As Richard Szafranski (1994, 1995) illuminated in his discussions of how information warfare ultimately becomes "neo-cortical warfare," the challenge for governments and societies becomes "epistemological." A netwar actor may aim to confound people's fundamental beliefs about the nature of their culture, society, and government, partly to foment fear but perhaps mainly to disorient people and unhinge their perceptions. This is why a netwar with a strong social content—whether waged by ethnonationalists, terrorists, or social activists—may tend to be about disruption more than destruction. The more epistemological the challenge, the more confounding it may be from an organizational standpoint. Whose responsibility is it to respond? Whose roles and missions are at stake? Is it a military, police, intelligence, or political matter? When the roles and missions of defenders are not easy to define, both deterrence and defense may become problematic.

Thus, the spread of netwar adds to the challenges facing the nation state in the information age. Its sovereignty and authority are usually exercised through bureacracies in which issues and problems can be sliced up and specific offices can be charged with taking care of specific problems. In netwar, things are rarely so clear. A protagonist is likely to operate in the cracks and gray areas of a society, striking where lines of authority crisscross and the operational paradigms of politicians, officials, soldiers, police officers, and related actors get fuzzy and clash. Moreover, where transnational participation is strong, a netwar's protagonists may expose a local government to challenges to its sovereignty and legitimacy by arousing foreign governments and business corporations to put pressure on the local government to alter its domestic policies and practices.

NETWORKS VERSUS HIERARCHIES: CHALLENGES FOR COUNTERNETWAR

These observations and the case studies presented in this volume lead to four policy-oriented propositions about the information revolution and its implications for netwar and counternetwar (Arquilla and Ronfeldt, 1993, 1996):[16]

Hierarchies have a difficult time fighting networks. There are examples of this across the conflict spectrum. Some of the best are found in the failings of many governments to defeat transnational criminal cartels engaged in drug smuggling, as in Colombia. The persistence of religious revivalist movements, as in Algeria, in the face of unremitting state opposition, shows both the defensive and offensive robustness of the network form. The Zapatista movement in Mexico, with its legions of supporters and sympathizers among local and transnational NGOs, shows that social netwar can put a democratizing autocracy on the defensive and pressure it to continue adopting reforms.

It takes networks to fight networks. Governments that want to defend against netwar may have to adopt organizational designs and strategies like those of their adversaries. This does not mean mirroring the adversary, but rather learning to draw on the same design principles that he has already learned about the rise of network forms in the information age. These principles depend to some extent on technological innovation, but mainly on a willingness to innovate organizationally and doctrinally, perhaps especially by building new mechanisms for interagency and multijurisdictional cooperation.

Whoever masters the network form first and best will gain major advantages. In these early decades of the information age, adversaries who are advanced at networking (be they criminals, terrorists, or peaceful social activists, including ones acting in concert with states) are enjoying an increase in their power relative to state agencies. While networking once allowed them simply to keep from being suppressed, it now allows them to compete on more nearly equal terms with states and other hierarchically oriented actors. The histories of

[16]Also see Berger (1998) for additional observations about such propositions.

Hamas and of the Cali cartel illustrate this; so do the Zapatista movement in Mexico and the International Campaign to Ban Landmines.

Counternetwar may thus require very effective interagency approaches, which by their nature involve networked structures. It is not necessary, desirable, or even possible to replace all hierarchies with networks in governments. Rather, the challenge will be to blend these two forms skillfully, while retaining enough core authority to encourage and enforce adherence to networked processes. By creating effective hybrids, governments may become better prepared to confront the new threats and challenges emerging in the information age, whether generated by ethnonationalists, terrorists, militias, criminals, or other actors. (For elaboration, see Arquilla and Ronfeldt, 1997, Ch. 19.)

However, governments tend to be so constrained by hierarchical habits and institutional interests that it may take some sharp reverses before a willingness to experiment more seriously with networking emerges. The costs and risks associated with failing to engage in institutional redesign are likely to be high—and may grow ever higher over time. In the most difficult areas—crime and terrorism—steps to improve intra- and international networking are moving in the right direction. But far more remains to be done, as criminal and terrorist networks continuously remake themselves into ever more difficult targets.

RECENT CASES OF NETWAR

Since we first wrote about netwar over seven years ago, there have been at least ten prominent (i.e., front-page) instances of its employment, in conflicts ranging from social activist campaigns to violent ethnic insurgencies (see Table 1.1). The netwar record has been generally successful. In these ten cases, which feature networked nonstate actors confronting states or groups of states, five netwars have achieved substantial success. Three have achieved limited success, while one (Burma) has yet to prove either a success or failure, and an-

Table 1.1

Prominent Cases of Netwar, 1994–2000

Campaign	Dates	Outcome	Type
Protracted Netwars			
EZLN[a]	1994–	Limited success	Autonomist
ICBL	1998–	Limited success	Globalist
Burma	1996–	Failing?	Mixed
Drug Cartels	1994–	Substantial success	Autonomist
Chechnya I	1994–1996	Substantial success	Autonomist
Chechnya II	1999–2000	Failure	Autonomist
Short-Duration Netwars			
Greenpeace	1994	Limited success	Globalist
Battle of Seattle	1999	Substantial success	Globalist
East Timor	1999	Substantial success	Autonomist
Serb Opposition	2000	Substantial success	Mixed

[a]Zapatista National Liberation Army.

other (Chechnya) must be judged, currently, as a failure.[17] Most of these cases, and the reasons for their success or the lack thereof, are discussed in detail in the following chapters.

The limits on some successes and the one failure imply a need to take a balanced view of netwar, analyzing the conditions under which it is most likely to succeed, fail, or fall somewhere in between. Clearly, there is enough success here to make netwar worth examining more closely. But it is important not to "tout" netwar, as Robert Taber (1970) once did guerrilla war. He was sharply rebutted by Lewis Gann (1970), who pointed out that guerrillas, far from being unstoppable, have of-

[17]Both Russo-Chechen conflicts are included as netwars, because of the extent to which the Chechens have relied upon networked forms of organization, both in field actions and in the struggle to win the "battle of the story." Arquilla and Karasik (1999) describe the Chechen victory in the 1994–1996 conflict as a clear triumph for networking but also posed concerns that the Russians would learn from this defeat—as they have learned from defeats throughout their history—and would improve, both in the field and in the arena of world perception. They have gotten better in the second conflict, driving the Chechens to their southern mountain redoubts and convincing state and nonstate actors around the world that Russian forces are fighting on behalf of a world community opposed to terrorism.

ten been defeated. Netwar will also have its ups and downs. Our purpose is to uncover and get a deeper understanding of its dynamics.

In Table 1.1, the cases are divided into those conflicts that were or have been drawn out, and those focused on specific crises—a useful distinction often made in studies of conflict. Interesting insights emerge. For example, the two most successful protracted campaigns were waged violently by ethnonationalists and criminals who sought freedom from state controls. The short-duration successes also included some use of violence (in two cases), and a global civil society reaction (that threatened a forceful response) to state violence in the other. And, though more muted, most of the other cases have violent aspects.

The table distributes netwars by type along a spectrum ranging from those that are globalist in orientation (e.g., the anti-landmine campaign), to those that are autonomist at the opposite end (e.g., the 1994 Chechen effort to secede from Russia). In the middle lie mixed cases where the objective is to gain power locally, but these netwars depend on the protagonists being able to open their societies to democratic, globalist influences.

The two unsuccessful netwar campaigns (in Russia and Burma) have featured networks confronting hierarchical authoritarian governments that have been willing to use substantial force to assert—in the case of Russia, to reassert—their hold on power. These networks' losses to hierarchies, combined with the fact that the principal successes to date have been gained by violent "uncivil society" actors, suggest being cautious about the claims for netwar. That said, the nonviolent International Campaign to Ban Landmines and the Greenpeace effort to curb nuclear testing both achieved reasonable measures of success without engaging in any violence whatsoever. This is a hopeful sign. And, while the civil society campaign to free Burma from authoritarian rule is a partial failure to date, this is a continuing campaign whose ultimate outcome is yet unknown.

Finally, these netwar conflicts feature an uneven split between those about globalist issues—aimed at fostering the rise of a rights- and ethics-based civil society—and the more frequent, somewhat darker "autonomist" variety of netwar, featuring nonstate actors trying to get

out from under state controls. Most of the limited successes that have been achieved thus far are globalist in orientation, while most of the substantial successes (save for the Battle of Seattle and Serbia) have been autonomist. It will be interesting, as the instances of netwar increase over time, to see whether this pattern holds. The outcomes of the globalist cases suggest the prevalence of negotiated solutions, while the autonomist conflicts may, in general, have a much more inherently desperate character that drives them to greater violence and less willingness to reach accommodation. All this we will watch in the years to come. For now, these early cases have helped us to develop this taxonomy of netwar, further refining the concept.

Will netwar continue to empower nonstate actors, perhaps reducing the relative power advantage enjoyed by nation states? Civil society networks have already made much use of social netwar as a tool for advancing a globalist, ethics-based agenda focused on broadening and deepening human rights regimes—often in the context of an ongoing effort to foster movement from authoritarian rule to democracy (e.g., Burma). But there is another side of nonstate-actor-oriented netwar, characterized not by globalist impulses, but rather by the desire to avoid state control of a network's criminal, terrorist, or ethnic-separatist agenda (e.g., Hamas and Chechens). While the globalist netwars seem devoted to nonviolent tools of struggle, the autonomists may employ both means of engagement—often with a greater emphasis on violence.

VARIETIES OF NETWAR—DUAL PHENOMENA

Netwar is a deduced concept—it derives from our thinking about the effects and implications of the information revolution. Once coined, the concept helps show that evidence is mounting about the rise of network forms of organization, and about the importance of "information strategies" and "information operations" across the spectrum of conflict, including among ethnonationalists, terrorists, guerrillas, criminals, and activists.[18] Note that we do not equate ethnonational-

[18]These are not the only types of netwar actors; there are others. For example, corporations may also engage in netwars—or find themselves on the receiving end of netwar campaigns.

ists, terrorists, guerrillas, criminals, and activists with each other—each has different dynamics. Nor do we mean to tarnish social activism, which has positive aspects for civil society.[19] We are simply calling for attention to a cross-cutting meta-pattern about network forms of organization, doctrine, and strategy that we might not have spotted, by induction or deduction, if we had been experts focused solely on any one of those areas.

Netwar can be waged by "good" as well as "bad" actors, and through peaceful as well as violent measures. From its beginnings, netwar has appealed to a broad cross-section of nonstate actors who are striving to confront or cope with their state authorities. Ethnonationalists, criminals, and terrorists—all have found new power in networking. But so too have emerging global civil society actors who have emphasized nonviolent efforts to win the "battle of the story"—a more purely informational dimension of netwar—rather than the violent swarming characteristic of its darker side. Both categories of actors seem to realize, even if only implicitly, that, in the future, conflict will become even more "irregularized," with the set-piece confrontations and battles of earlier eras largely disappearing. While the U.S. military remains focused—in terms of budgetary emphasis, doctrine, and force structure—on the traditional forms of conflict, the rise of netwar should prompt a shift to a nimble "turn of mind," one far less attuned to fighting in the Fulda Gap or the Persian Gulf and more focused on engaging a range of odd new adversaries across a densely interconnected "global grid."

The duality of netwar in the real world—dark-side criminals and terrorists on the one hand, but enlightening civil society forces on the other—is mirrored in the virtual world of cyberspace, which is increasingly utilized for crime and terror (still embryonic), along with social activism. At present, social activism is far more robust and established in the cyber realm than is crime or terror. Will this continue to be the case? We think so. Activists will become more adept at integrating the mobilizing force of the Internet with the power and appeal of messages aimed at spreading and protecting human rights. Even

[19]See discussion in Ronfeldt (1996).

so, criminal and terrorist organizations will learn how to manipulate the infosphere with increasing skill.

Thus, netwar has two faces, like the Roman god Janus. Janus was the god of doors and gates, and thus of departures and returns, and new beginnings and initiatives. This, in a sense, meant he was the god of communications, too. His double face, one old and looking back, the other younger and peering forward, conveyed that he was an inherently dual god. At the beginning of creation, he partook in the separation of order from chaos. In Roman times, he was identified with the distinction between war and peace, for the gate to his temple at the Forum was kept ceremoniously closed in times of peace and open in times of war—which meant the gates were rarely closed. At the start of the 21st century, the world is again at a new beginning. It is uncertain whether it will be an era of peace or conflict; but how matters turn out will depend to some degree on which face of netwar predominates.

This volume explores the two faces of netwar, in three parts. The first part is composed of three chapters that chronicle the increasingly networked nature of major types of "uncivil-society" actors for whom violence is a principal mode of expression. The analyses by Michele Zanini and Sean Edwards of Arab terrorist groups, by Phil Williams of transnational criminal networks, and by John Sullivan of street-level gangs and hooligans, all speak to the increasingly sophisticated usage of the new information technologies to enhance both these groups' organizational and operational capabilities.

The second part of the book examines the rise of social netwar, again with three chapters. These chapters examine social netwars waged by networked civil society actors against various types of states. Tiffany Danitz and Warren Strobel show the limitations (but also some successful facets) of social netwar when waged against a resolute dictatorship that maintains a system virtually closed to civil society. Our own chapter on Mexico finds that an "NGO swarm" was quite effective in transforming a rural insurgency into a mostly peaceable netwar in a then rather authoritarian system. Paul de Armond provides insights into the full mobilizing potential of social netwar when conducted in a free society like the United States.

The final part considers the future of netwar, particularly regarding how technology, organization, and doctrine interact. Dorothy Denning assesses whether activists, hacktivists, or cyberterrorists may gain the most influence from exploiting the new information technologies. Luther Gerlach's chapter, though focused on environmental activism, identifies the dynamics of organizations that are segmentary, polycentric, and integrated as a network—from leaderlessness to operational fluidity. We think these dynamics apply, in varying degrees, to all the types of actors examined in the first two parts of the book. Our concluding chapter addresses likely trends in both the theory and practice of netwar—from how to draw on academic theories about networks, to how to think strategically about netwar itself. Thus, Part III should make the reader aware of both the perils and the promises of netwar, while also providing analytical guideposts for future studies of this phenomenon.

BIBLIOGRAPHY

Arquilla, John, and Theodore Karasik, "Chechnya: A Glimpse of Future Conflict?" *Studies in Conflict and Terrorism*, Vol. 22, No. 3, July–September 1999, pp. 207–230.

Arquilla, John, and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy,* Vol. 12, No. 2, Summer 1993, pp. 141–165. Available as RAND reprint RP-223.

Arquilla, John, and David Ronfeldt, *The Advent of Netwar,* Santa Monica, Calif.: RAND, MR-789-OSD, 1996.

Arquilla, John, and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy,* Santa Monica, Calif.: RAND, MR-1033-OSD, 1999.

Arquilla, John, and David Ronfeldt, *Swarming and the Future of Conflict*, Santa Monica, Calif.: RAND, DB-311-OSD, 2000.

Arquilla, John, and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1997.

Arquilla, John, David Ronfeldt, and Michele Zanini, "Information-Age Terrorism and the U.S. Air Force," in Ian O. Lesser et al., *Countering the New Terrorism,* Santa Monica, Calif.: RAND, MR-989-AF, 1999.

Beam, Louis, "Leaderless Resistance," *The Seditionist*, Issue 12, February 1992 (text can also be located sometimes on the web).

Berger, Alexander, *Organizational Innovation and Redesign in the Information Age: The Drug War, Netwar, and Other Low-End Conflict,* master's thesis, Monterey, Calif.: Naval Postgraduate School, 1998.

Bonabeau, Eric, Marco Dorigo, and Guy Theraulaz, *Swarm Intelligence: From Natural to Artificial Systems,* Oxford: Oxford University Press, 1999.

Bowden, Mark, *Blackhawk Down: A Story of Modern War,* New York: Atlantic Monthly Press, 1999.

Brin, David, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, Mass.: Addison-Wesley, 1998.

Castells, Manuel, *The Information Age: Economy, Society and Culture,* Vol. II, *The Power of Identity,* Malden, Mass.: Blackwell Publishers, 1997.

Cleaver, Harry, "The Zapatistas and the Electronic Fabric of Struggle," 1995, www.eco.utexas.edu/faculty/Cleaver/zaps.html, printed in John Holloway and Eloina Pelaez, eds., *Zapatista! Reinventing Revolution in Mexico*, Sterling, Va.: Pluto Press, 1998, pp. 81–103.

Cleaver, Harry, "The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric," *Journal of International Affairs*, Vol. 51, No. 2, Spring 1998, pp. 621–640.

Cleaver, Harry, *Computer-Linked Social Movements and the Global Threat to Capitalism,* July 1999, www.eco.utexas.edu/faculty/Cleaver/polnet.html.

Edwards, Sean J.A., *Swarming on the Battlefield: Past, Present and Future,* Santa Monica, Calif.: RAND, MR-1100-OSD, 2000.

Evan, William M., "An Organization-Set Model of Interorganizational Relations," in Matthew Tuite, Roger Chisholm, and Michael Rad-

nor, eds., *Interorganizational Decisionmaking*, Chicago: Aldine Publishing Company, 1972, pp. 181–200.

Gann, Lewis, *Guerrillas in History,* Stanford, Calif.: Hoover Institution Press, 1970.

Gerlach, Luther P., "Protest Movements and the Construction of Risk," in B. B. Johnson and V. T. Covello, eds., *The Social and Cultural Construction of Risk*, Boston: D. Reidel Publishing Co., 1987, pp. 103–145.

Gerlach, Luther P., and Virginia Hine, *People, Power, Change: Movements of Social Transformation,* New York: The Bobbs-Merrill Co., 1970.

Gray, Chris Hables, *Postmodern War: The New Politics of Conflict*, New York: The Guilford Press, 1997.

Kelly, Kevin, *Out of Control: The Rise of Neo-Biological Civilization,* New York: A William Patrick Book, Addison-Wesley Publishing Company, 1994.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, and Brian Jenkins, *Countering the New Terrorism*, Santa Monica, Calif.: RAND, MR-989-AF, 1999.

Nye, Joseph S., *Bound to Lead: The Changing Nature of American Power,* New York: Basic Books, 1990.

Nye, Joseph S., and William A. Owens, "America's Information Edge," *Foreign Affairs,* Vol. 75, No. 2, March/April 1996, pp. 20–36.

Ronfeldt, David, *Tribes, Institutions, Markets, Networks—A Framework About Societal Evolution,* Santa Monica, Calif.: RAND, P-7967, 1996.

Ronfeldt, David, John Arquilla, Graham Fuller, and Melissa Fuller, *The Zapatista "Social Netwar" in Mexico*, Santa Monica, Calif.: RAND, MR-994-A, 1998.

Szafranski, Colonel Richard, "Neo-Cortical Warfare? The Acme of Skill," *Military Review*, November 1994, pp. 41–55.

Szafranski, Colonel Richard, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal*, Spring 1995, pp. 56–65.

Taber, Robert, *The War of the Flea*, New York: Citadel, 1970.

Toffler, Alvin, and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-First Century*, Boston: Little, Brown and Company, 1993.

Van Creveld, Martin, *The Transformation of War*, New York: Free Press, 1991.

Wehling, Jason, *"Netwars" and Activists Power on the Internet,* March 25, 1995—as circulated on the Internet (and once posted at www.teleport.com/~jwehling/OtherNetwars.html).

Williams, Jody, and Stephen Goose, "The International Campaign to Ban Landmines," in Maxwell A. Cameron, Robert J. Lawson, and Brian W. Tomlin, eds., *To Walk Without Fear: The Global Movement to Ban Landmines*, New York: Oxford University Press, 1998, pp. 20–47.

Wray, Stefan, *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics,* paper for a conference on The World Wide Web and Contemporary Cultural Theory, Drake University, November 1998, www.nyu.edu/projects/wray/wwwhack.html.